Justin L. James (15167)
JAMES DODGE RUSSELL & STEPHENS
10 West Broadway, Suite 400
Salt Lake City, Utah 84101
Telephone: 801.363.6363
Email: jjames@jdrslaw.com

Gary M. Klinger*
gklinger@milberg.com
Milberg Coleman Bryson Phillips Grossman PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878

*Pro Hac Vice Forthcoming

Attorneys for Plaintiffs and Proposed Class Counsel

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

NICK PEPPELAAR and TARA SCHULMEISTER, on behalf of themselves individually and on behalf of all others similarly situated, **Plaintiffs,** **v.** **SNAP FINANCE LLC and SNAP RTO LLC,** **Defendants.**	**COMPLAINT** **[PROPOSED CLASS ACTION]** **JURY TRIAL DEMANDED** **Case No.: 2:23-cv-00064**

INTRODUCTION

Plaintiffs Nick Peppelaar and Tara Schulmeister ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendants Snap Finance, LLC and Snap RTO LLC (collectively, "Snap" or "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

1. This class action arises out of the recent data breach ("Data Breach") involving Defendants, which are Utah-based companies that provide their customers with financing for a variety of purchases allowing them to "[g]et it now, pay later – with worry-free lease-to-own financing".[1]

2. Plaintiffs bring this Complaint against Defendants for their failure to properly secure and safeguard the personally identifiable information that they collected and maintained as part of their regular business practices, including, but not limited to, names, Social Security numbers, driver's license numbers, and financial account numbers (collectively defined herein as "PII").

3. Upon information and belief, former and current Snap customers are required to entrust Defendants with sensitive, non-public PII, without which Defendants could not perform their regular business activities, in order to apply for financing from Snap. Defendants retain this information for at least many years and even after the consumer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. "Earlier this year" in 2022, Defendants became aware of suspicious activity on their network. Defendants proceeded to investigate the nature and scope of the suspicious activity and subsequently concluded that "there was unauthorized access to our environment between June 23,

[1] https://snapfinance.com/

and September 8, 2022" and that "an unauthorized actor had the ability to access certain information stored on the network during this period of time."[2]

6. According to Defendants' Notice of Security Incident letter (the "Notice Letter"), the compromised PII included individuals' names, Social Security numbers, driver's license numbers or state identification number, and financial account number.[3]

7. Defendants' investigation concluded that the PII compromised in the Data Breach included Plaintiffs' and approximately 61,000 other individuals' information.[4]

8. Defendants failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Moreover, although Defendants did not disclose the date that Snap learned of the Data Breach, Snap did disclose that the investigation determined on October 28, 2022 that the "data contained certain information related to" Plaintiffs and Class Members.

---

[2] The "Notice Letter". A copy of the letter is available at https://ago.vermont.gov/blog/2022/12/02/snap-finance-data-breach-notice-to-consumers/?utm_source=rss&utm_medium=rss&utm_campaign=snap-finance-data-breach-notice-to-consumers

[3] *Id.*

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/d193f4eb-a877-4395-9a3c-8b94833c907c.shtml

10. Nonetheless, Snap did not notify Plaintiffs and Class Members of the Data Breach and/or inform them that their PII was compromised until nearly six weeks later. Since the date the Data Breach started, on June 23, 2022, Plaintiffs and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

11. In breaching their duties to properly safeguard customers' PII and give customers timely, adequate notice of the Data Breach's occurrence, Defendants' conduct amounts to negligence and/or recklessness and violates federal and state statutes.

12. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

13. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a

continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. Plaintiffs and Class Members have suffered injuries as a result of Defendants' conduct. These injuries include: (i) fraudulent charges to their credit and/or debit cards; (ii) time spent opening and closing financial accounts; (iii) damage to their credit scores; (iv) time spent corresponding with Defendants, credit bureaus, and their banks; (v) time spent enrolling in credit and identity theft monitoring insurance; (vi) changing passwords and resecuring their own computers; (vii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

15. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

PARTIES

16. Plaintiff Peppelaar is and has been, at all relevant times, a resident and citizen of Utah, currently residing in Kerns, Utah Mr. Peppelaar received the Notice Letter, via U.S. mail, directly from Defendants, dated December 1, 2022

17. Mr. Peppelaar provided his PII to Defendants on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable safeguards to protect his PII. If Mr. Peppelaar had known that Defendants would not adequately protect his PII, he would not have entrusted Defendants with his PII or allowed Defendants to maintain this sensitive PII.

18. Plaintiff Schulmeister is and has been, at all relevant times, a resident and citizen of Ohio, currently residing in Akron, Ohio. Ms. Schulmeister received the Notice Letter, via U.S. mail, directly from Defendants, dated December 1, 2022

19. Ms. Schulmeister provided her PII to Defendants on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable safeguards to protect her PII. If Ms. Schulmeister had known that Defendants would not adequately protect her PII, she would not have entrusted Defendants with her PII or allowed Defendants to maintain this sensitive PII.

20. Defendant Snap Finance LLC is a company that provides financing to consumers for a variety of purchases. Defendant Snap Finance LLC is incorporated under the laws of the state of Utah, with its principal office located at 1275 West 2240 South, West Valley, UT 84119.

21. Defendant Snap RTO LLC offers lease-to-own financing to retail consumers through partnerships with merchants and retailers. Defendant Snap RTO LLC is incorporated under the laws of the state of Utah and maintains its principal place of business at 1193 West 2400 South Salt Lake City, Utah 84119.

22. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein

are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

23. All of Plaintiffs' claims stated herein are asserted against Snap and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

24. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

25. All of Plaintiffs' claims stated herein are asserted against Snap and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff Schulmeister, is a citizen of a state different from Defendants.

27. This Court has personal jurisdiction over Defendants because their principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

28. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendants' principal place of business is in this District.

BACKGROUND

29. Defendants are a Utah-based company that provides its customers with financing for a variety of purchases that allows them to "[g]et it now, pay later – with worry-free lease-to-own financing".[5]

30. Plaintiffs and Class Members are current and former Snap customers who used Snap to finance one or more purchases.

31. In order to apply for financing at Snap, Plaintiffs and Class Members were required to provide sensitive and confidential PII, including their names, dates of birth, Social Security numbers, driver's license numbers, financial information, and other sensitive information.

32. The information held by Defendants in their computer systems included the unencrypted PII of Plaintiffs and Class Members.

33. Upon information and belief, Defendants made promises and representations to its customers, including Plaintiffs and Class Members, that the PII collected from them as a condition of submitting an application for financing would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after it was no longer required to maintain it.

[5] https://snapfinance.com/

34. Indeed, Defendants' Privacy Policy provides that: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[6]

35. Plaintiffs and Class Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

36. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

37. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendants has a legal duty to keep consumer's PII safe and confidential.

38. Defendants had obligations created by FTC Act, the Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

39. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

[6] https://snapfinance.com/legal/privacy

40. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

THE DATA BREACH

41. On or about December 1, 2022, Defendants began sending Plaintiffs and other victims of the Data Breach a Notice of Data Event letter, informing them that:

> Earlier this year, Snap discovered suspicious activity in its environment. Upon learning this, Snap immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that there was unauthorized access to our environment between June 23, 2022 and September 8, 2022. The investigation also determined that an unauthorized actor had the ability to access certain information stored on the network during this period of time. Therefore, Snap undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and whom it related. On October 28, 2022, Snap completed this review and determined the data contained certain information related to you.[7]

42. Omitted from the Notice Letter were the date that Defendants discovered the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, why it took over a month to inform impacted individuals after Defendants determined their information was involved, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

43. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without

[7] *Notice Letter.*

these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

44. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

45. The attacker accessed and acquired files in Defendants' computer systems containing unencrypted PII of Plaintiffs and Class Members, including their names, Social Security numbers, driver's license numbers, and financial account information. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

46. Plaintiffs further believe their PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

DATA BREACHES ARE PREVENTABLE

47. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

48. To prevent and detect cyber-attacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Government, the following measures:

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

49. To prevent and detect cyber-attacks Snap could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

[9] *Id.* at 3-4.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[10]4.

50. To prevent and detect cyber-attacks or ransomware attacks Snap could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection

[10] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Oct. 17, 2022).

- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[11]

51. Given that Defendants were storing the sensitive PII of its current and former customers, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

52. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of over 61,000 customers, including that of Plaintiffs and Class Members.

SNAP ACQUIRES, COLLECTS, AND STORES PLAINTIFFS' PII

53. As a condition to obtain financing from Snap, Plaintiffs and Class Members were required to give their sensitive and confidential PII to Defendants.

54. Defendants retain and store this information and derive a substantial economic benefit from the PII that they collect. But for the collection of Plaintiffs' and Class Members' PII, Defendants would be unable to perform financing services.

55. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

56. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

57. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

58. Upon information and belief, Defendants made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

59. Indeed, Defendants' Privacy Policy provides that: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[12]

60. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

SNAP KNEW, OR SHOULD HAVE KNOWN, OF THE RISK BECAUSE FINANCING COMPANIES IN POSSESSION OF PII ARE PARTICULARLY SUSCEPTIBLE TO CYBER ATTACKS

61. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

62. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendants, preceding the date of the breach.

[12] https://snapfinance.com/legal/privacy

63. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

64. Additionally, as companies became more dependent on computer systems to run their business,[13] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[14]

65. As a custodian of PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

66. Indeed, Defendants' Privacy Policy evidences its knowledge of the foreseeable risks of Data Breaches, like the one it experienced, stating that it uses customers' Personal Information for "[d]etecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity."[15]

[13]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html
[14] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022
[15] https://snapfinance.com/legal/privacy

67. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[16]

68. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[17]

69. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

70. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[18]

71. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

---

[16] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[17] *Id*.

[18] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

72. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s), amounting to potentially thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

73. In the Notice Letter, Defendants makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

74. Defendants' offering of credit and identity monitoring establishes that Plaintiffs and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendants' computer systems.

75. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

76. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

77. As a financing company in possession of its customers' and former customers' PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them

by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

VALUE OF PERSONALLY IDENTIFYING INFORMATION

78. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

79. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[21] For example, Personal Information can be sold at a price ranging from $40

[19] 17 C.F.R. § 248.201 (2013).
[20] *Id.*
[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

to $200.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

80. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[24]

81. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[22] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

82. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

83. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[26]

85. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

86. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 17, 2022).

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

87. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

SNAP FAILS TO COMPLY WITH FTC GUIDELINES

88. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

89. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

[27] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[28]

90. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[29]

91. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

93. These FTC enforcement actions include actions against financing companies, like Defendants. *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 408

[28] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).
[29] *Id.*

(E.D. Va. 2020) *("*"Plaintiffs have plausibly alleged a claim" based upon violation of Section 5 of the FTC Act.)

94. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

95. Defendants failed to properly implement basic data security practices.

96. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

97. Upon information and belief, Snap was at all times fully aware of its obligation to protect the PII of its customers, Snap was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

SNAP VIOLATED THE GRAMM-LEACH-BLILEY ACT

98. Snap is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

99. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

100. Defendants collect nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendants were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

101. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

102. Accordingly, Defendants' conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

103. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality

policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendants violated the Privacy Rule and Regulation P.

104. Defendants failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendants' network systems.

105. Defendants failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

106. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes

to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendants violated the Safeguard Rule.

107. Defendants failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

108. Defendants violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class Members with a non-affiliated third party without providing Plaintiffs and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

SNAP FAILS TO COMPLY WITH INDUSTRY STANDARDS

109. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

110. Several best practices have been identified that, at a minimum, should be implemented by financing companies in possession of PII, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Snap failed to follow these industry best practices, including a failure to implement multi-factor authentication.

111. Other best cybersecurity practices that are standard in the financing industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as

firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Snap failed to follow these cybersecurity best practices, including failure to train staff.

112. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

113. These foregoing frameworks are existing and applicable industry standards in the financing industry, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

114. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of

benefit of the bargain (price premium damages); (g) diminution of value of their Private Information; and (i) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Snap fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

THE DATA BREACH INCREASES PLAINTIFFS' & CLASS MEMBERS' RISK OF IDENTITY THEFT

115. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

116. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

117. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

118. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

LOSS OF TIME TO MITIGATE THE RISK OF IDENTITY THEFT AND FRAUD

119. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn

about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

120. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendants' Notice Letter encourages them, monitor their financial accounts for many years to mitigate the risk of identity theft.

121. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as contacting Defendants regarding a fraudulent purchase made through Snap; contacting a merchant regarding a fraudulent purchase; contacting banks regarding fraudulent activity on their credit and/or debit cards; contacting credit bureaus about the Data Breach and fraudulent activity; enrolling in credit and identity theft monitoring insurance; and changing passwords and resecuring their own computers.

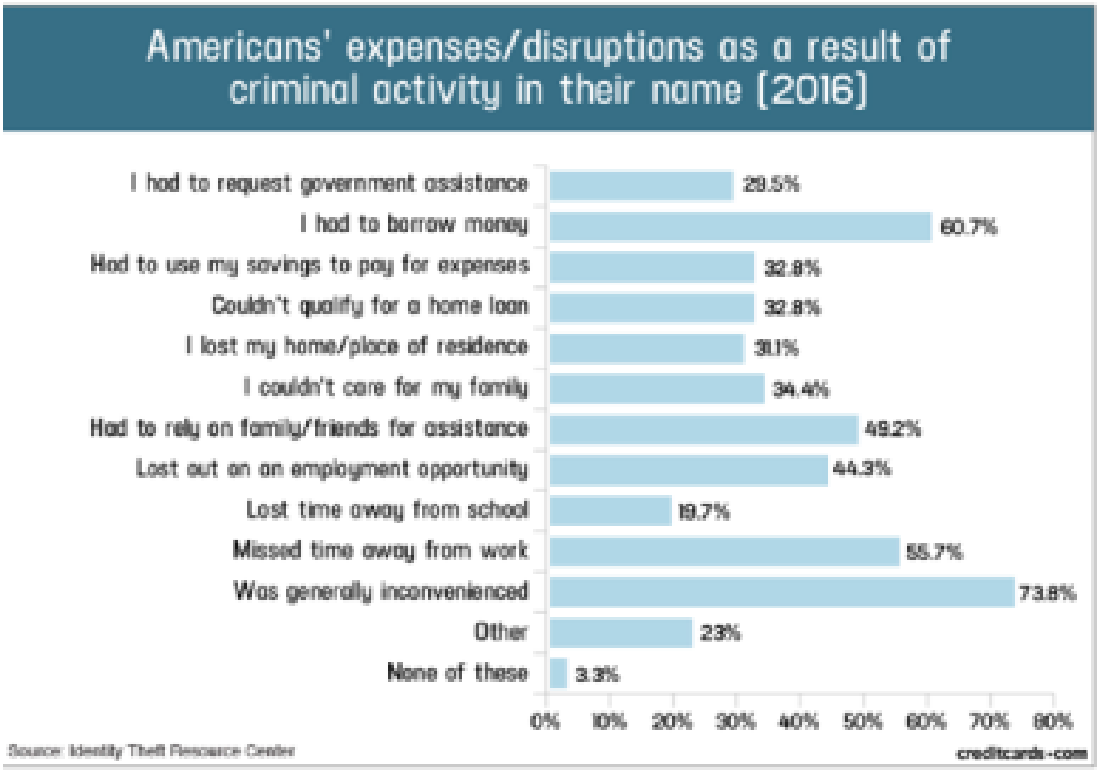
122. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

123. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity),

[30] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

124. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[32]



125. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

[31] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[32] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).

DIMINUTION OF VALUE OF PII

126. PII is a valuable property right.[33] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

127. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[34]

128. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[35] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[36,37] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[38]

129. As a result of the Data Breach, Plaintiffs' and Class Members' PII , which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by

---

[33] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").
[34] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[35] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).
[36] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[37] https://datacoup.com/
[38] https://digi.me/what-is-digime/

its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

130. Driver's license numbers are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[39]

131. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[40]

132. According to cybersecurity specialty publication CPO Magazine, "[t]o

[39] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[40] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) (last accessed July 20, 2021)

those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[41] However, this is not the case. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[42]

133. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[43]

134. At all relevant times, Snap knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

135. The fraudulent activity resulting from the Data Breach may not come to light for years.

136. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

---

[41] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021)
[42] *Id.*
[43] *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021)

137. Snap was, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to potentially hundreds of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

138. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

FUTURE COST OF CREDIT AND IDENTITY THEFT MONITORING IS REASONABLE AND NECESSARY

139. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

140. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

141. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

142. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendants' failure to safeguard their PII .

LOSS OF BENEFIT OF THE BARGAIN

143. Furthermore, Defendants' poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendants for financing, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII , when in fact, Snap did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

PLAINTIFF PEPPELAAR'S EXPERIENCE

144. Plaintiff Peppelaar obtained financing from Snap to purchase automobile tires in or about 2018. In order to obtain financing services from Defendants, he was required to provide his PII to Defendants.

145. At the time of the Data Breach—from June 23, 2022 through September 8, 2022–– Snap retained Plaintiff's' PII in its system.

146. Plaintiff Peppelaar is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

147. Plaintiff Peppelaar received the Notice Letter, by U.S. mail, directly from Defendants, dated December 1, 2022. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, financial account number, and driver's license number.

148. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, Plaintiff Peppelaar made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; reporting fraudulent activity to Defendants and the merchant involved; corresponding with credit bureaus; cancelling his debit card; and switching financial institutions. Plaintiff Peppelaar has spent significant time dealing with the Data Breach, valuable time Plaintiff Peppelaar otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

149. Plaintiff Peppelaar suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) fraudulent charges to his credit and/or debit cards; (ii) time spent opening and closing financial accounts; (iii) damage to his credit score; (iv) time spent corresponding with Defendants, credit bureaus, and their banks about the Data Breach's occurrence and the fraudulent activity resulting from it; (v) time spent enrolling in credit and identity theft monitoring insurance; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized

third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails

150. The Data Breach has caused Plaintiff Peppelaar to suffer fear, anxiety, and stress, which has been compounded by the fact that Snap has still not fully informed him of key details about the Data Breach's occurrence.

151. As a result of the Data Breach, Plaintiff Peppelaar anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Peppelaar is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

152. Plaintiff Peppelaar has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Defendants' possession, is protected and safeguarded from future breaches.

PLAINTIFF SCHULMEISTER'S EXPERIENCE

153. Plaintiff Schulmeister obtained financing from Snap to purchase earrings in or about 2020. In order to obtain financing services from Defendants, she was required to provide her PII to Defendants.

154. At the time of the Data Breach—from June 23, 2022 through September 8, 2022–– Snap retained Plaintiff Schulmeister's PII in its system.

155. Plaintiff Schulmeister is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

156. Plaintiff Schulmeister received the Notice Letter, by U.S. mail, directly from Defendants, dated December 1, 2022. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, financial account number, and driver's license number.

157. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, Plaintiff Schulmeister made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; reporting fraudulent activity on her financial accounts; changing passwords and resecuring her own computer system; and researching the credit monitoring and identity theft insurance services offered by Defendant; and enrolling in the credit monitoring and identity theft insurance services. Plaintiff has spent approximately twenty hours on remedying the breach—time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

158. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to, (i) fraudulent purchases under her name; (ii) invasion of privacy; (iii) time spent enrolling in credit and identity theft monitoring insurance; (iv) changing passwords and resecuring her own computers; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vi) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants'

possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

159. The Data Breach has caused Plaintiff Schulmeister to suffer fear, anxiety, and stress, which has been compounded by the fact that Snap has still not fully informed her of key details about the Data Breach's occurrence.

160. As a result of the Data Breach, Plaintiff Schulmeister anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Schulmeister is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

161. Plaintiff Schulmeister has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

162. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

163. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendants on or about December 1, 2022 (the "Class").

164. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

165. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

166. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 60,000 individuals were notified by Defendants of the Data Breach, according to the breach report submitted to Maine Attorney General's Office.[44] The Class is apparently identifiable within Defendants' records, and Defendants has already identified these individuals (as evidenced by sending them breach notification letters).

167. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

[44] https://apps.web.maine.gov/online/aeviewer/ME/40/d193f4eb-a877-4395-9a3c-8b94833c907c.shtml

c. Whether Defendants had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

168. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

169. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

170. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

171. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for

those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

172. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

173. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

174. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

175. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

176. Further, Defendants has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

177. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT ONE

NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

178. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

179. Defendants require their customers, including Plaintiffs and Class Members to submit non-public Private Information in the ordinary course of providing financing services.

180. Plaintiffs and Class Members entrusted Defendants with their Private Information for the purpose of securing financial services from Defendants.

181. Snap owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

182. Snap had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

183. Defendants' duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

184. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Snap and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Snap with their confidential PII, a necessary part of being customers of Defendants.

185. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Snap is bound by industry standards to protect confidential Private Information.

186. Snap was subject to an "independent duty," untethered to any contract between Snap and Plaintiffs or the Class.

187. Snap also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

188. Snap also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Class.

189. Snap breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Snap include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

190. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

191. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in both the financial services and medical industry.

192. Snap has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

193. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Snap knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

194. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

195. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

196. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

197. Snap had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

198. Snap has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

199. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

200. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

201. Snap violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

202. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

203. Snap violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendants' internal systems that were inadequately secured and accessible to unauthorized third-parties from the internet, (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system, (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information, (d) failed to adequately (i) test and/or monitor the system where the Data Breach occurred and (ii) update and/or further secure its data security practices in light of the heightened risk environment.

204. Defendants' violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes negligence.

205. Plaintiffs and the Class are within the class of persons that the FTC Act and the GLBA were intended to protect.

206. Defendants' violation of the GLBA and FTC Act is prima facie evidence of negligence.

207. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

208. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) fraudulent charges to their credit and/or debit cards; (ii) time spent opening and closing financial accounts; (iii) damage to their credit scores; (iv) time spent corresponding with Defendants, credit bureaus, and their banks; (v) time spent enrolling in credit and identity theft monitoring insurance; (vi) changing passwords and resecuring their own computers; (vii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails.

209. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

210. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as

Snap fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

211. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

212. Defendants' negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

213. Plaintiffs and Class Members are also entitled to injunctive relief requiring Snap to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT TWO

UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

214. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

215. Plaintiffs and Class Members conferred a monetary benefit to Defendants when they provided their PII and payment for Defendants' financial services.

216. Defendants knew that Plaintiffs and Class Members conferred a monetary benefit to Defendants and they accepted and retained that benefit. Defendants profited from this monetary benefit, as the transmission of PII to Defendants from Plaintiffs and Class Members is an integral part of Defendants' business. Without collecting and maintaining Plaintiffs' and Class Members' PII, Defendants would be unable to offer financial services.

217. Defendants were supposed to use some of the monetary benefit provided to it by Plaintiffs and Class Members to secure the PII belonging to Plaintiffs and Class Members by paying for costs of adequate data management and security.

218. Defendants should not be permitted to retain any monetary benefit belonging to Plaintiffs and Class Members because Defendants failed to implement necessary security measures to protect the Private Information of Plaintiffs and Class Members.

219. Defendants gained access to the Plaintiffs' and Class Members' PII through inequitable means because Defendants failed to disclose that it used inadequate security measures.

220. Plaintiffs and Class Members were unaware of the inadequate security measures and would not have entrusted their Private Information to Defendants had they known of the inadequate security measures.

221. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiffs and Class Members have no adequate remedy at law.

222. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants'

possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

223. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

224. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds from the monetary benefit that it unjustly received from them.

COUNT THREE

INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

225. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

226. The State of Utah recognizes the tort of Invasion of Privacy:

> The elements of an invasion-of-privacy claim are: (1) the disclosure of the private facts must be a public disclosure and not a private one; (2) the facts disclosed to the public must be private facts, and not public ones; (3) the matter made public must be one that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities. *Shattuck-Owen v. Snowbird Corp*, 2000 UT 94, 16 P.3d 555 (2000) (citing *Stein v. Marriott Ownership Resorts, Inc.*, 944 P.2d 374, 380 (Utah Ct.App.1997) (quoting W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 117, at 856-57 (5th ed.1984) (footnote omitted)).

227. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Snap disclosed as a result of the Data Breach.

228. Defendants' conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

229. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by willfully failing to take reasonable precautions to avoid the disclosure of said information to unauthorized parties for unauthorized use, Snap intentionally invaded Plaintiffs' and Class Members' privacy by intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person; and intentionally causing anguish or suffering to Plaintiffs and Class Members.

230. Snap knew that an ordinary person in Plaintiffs' or a Class Member's position would consider Defendants' intentional actions or omissions highly offensive and objectionable.

231. Snap invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' seclusion by willfully failing to take reasonable precautions to avoid the disclosure of the Private Information of Plaintiffs and the Class Members without their informed, voluntary, affirmative, and clear consent.

232. Snap intentionally concealed from Plaintiffs and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

233. As a proximate result of such mishandling and disclosure of Private Information, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was

unduly frustrated and thwarted. Snap's conduct, amounting to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

234. In failing to protect Plaintiffs' and Class Members' Private Information, and willfully failing to take reasonable precautions to avoid the disclosure of the Private Information, Snap acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts

described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Snap can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect Themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to the Seventh Amendment to the Constitution of the United States of America, Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: January 25, 2023

Respectfully Submitted,

By: /s/ *Justin L/ James*
Justin L. James

Justin L. James (15167)
JAMES DODGE RUSSELL & STEPHENS
10 West Broadway, Suite 400
Salt Lake City, Utah 84101
Telephone: 801.363.6363
Email: jjames@jdrslaw.com

Gary M. Klinger*
gklinger@milberg.com
Milberg Coleman Bryson
Phillips Grossman PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878

Attorneys for Plaintiffs and
Proposed Class Counsel

*Pro Hac Vice Forthcoming